

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Missouri

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 THE PREMISES LOCATED AT:  
 276 ASPEN VILLAGE DRIVE, BALLWIN, MISSOURI 63021,  
 LOCATED IN THE EASTERN DISTRICT OF MISSOURI

Case No. 4:21 MJ 8335 SRW

SIGNED AND SUBMITTED TO THE COURT  
FOR FILING BY RELIABLE ELECTRONIC MEANS

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Section 2251	Production of Child Pornography
18 U.S.C. Section 2252	Receipt, Distribution and Possession of Child Pornography
18 U.S.C. Section 2252A	Receipt, Distribution and Possession of Child Pornography
18 U.S.C. Section 2422	Online Enticement and Solicitation of Sex with a Minor

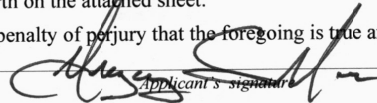
The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

☒ Continued on the attached sheet.

☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

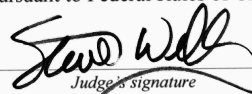
I state under the penalty of perjury that the foregoing is true and correct.



Gregory S. Marx, Special Agent, FBI

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: October 20, 2021


Judge's signature

City and state: St. Louis, MO

Stephen R. Welby, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF                    )  
THE PREMISES LOCATED AT:                            ) No. 4:21 MJ 8335 SRW  
276 ASPEN VILLAGE DRIVE, BALLWIN,                )  
MISSOURI 63021, LOCATED IN THE                    )  
EASTERN DISTRICT OF MISSOURI                    ) FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Gregory S. Marx, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 276 ASPEN VILLAGE DR., BALLWIN, MISSOURI 63021, further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation's ("FBI") Crimes Against Children Task Force. I have been an FBI agent for over 13 years. I have conducted numerous investigations regarding the sexual exploitation of children that involve the use of a computer which has been used to commit a crime in violation of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422 and 2423. As an FBI Special Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been personally involved in the execution of search warrants to search residences and seize material relating to the sexual exploitation of minors including computers, computer equipment, software, and electronically stored information. I have

experience utilizing computers during my career as an investigator and I have completed multiple in-service trainings and other courses in computer crime investigation.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from local law enforcement and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422 (the “SUBJECT OFFENSES”) have been committed by **LUKE EDWARD NICOZINSIN**, or other persons known and unknown. Section 2251 criminalizes the production of child pornography. Sections 2252 and 2252A criminalize, among other things, the receipt, distribution, and possession of child pornography. Section 2422 criminalizes the online enticement and solicitation of sex with a minor. There is also probable cause to search the premises described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

#### **LOCATION TO BE SEARCHED**

5. The location to be searched (the “SUBJECT PREMISES”) is: 276 ASPEN VILLAGE DR., BALLWIN, MISSOURI 63021, further described as: a single-family residence, with “276” clearly marked on the mailbox and above the garage door, and includes the residential building, any vehicles in the garage and/or driveway (including but not limited to a 2003 Nissan 350, Missouri plate FR0H4N). The SUBJECT PREMISES is further described in the Attachment A, and the accompanying photograph of the premises.

### **DEFINITIONS**

6. The following terms have the indicated meaning in this affidavit:

a. The term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device. 18 U.S.C. § 1030(e). The term computer included cellular telephones.

b. The term “minor” means any individual under the age of 18 years. 18 U.S.C. § 2256(1).

c. “Sexually explicit conduct” means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the anus, genitals, or pubic area of any person. 18 U.S.C. § 2256(2)(A).

d. “Visual depiction” includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 U.S.C. § 2256(5).

e. “Child pornography” includes any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit

conduct or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 U.S.C. § 2256(8)(A) or (C).

f. “Identifiable minor” means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person’s face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 U.S.C. § 2256(9).

g. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including for example, tablets, digital music devices, portable electronic game systems, electronic game consoles and wireless telephones. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer

software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

k. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory

calculators, electronic dialers, electronic notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

l. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

m. “Wireless telephone or mobile telephone, or cellular telephone” as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

#### **BACKGROUND RELATING TO SNAPCHAT**

7. The Internet is in part a computer communications network using interstate and foreign telephone and communication lines to transmit data streams, including data streams used

to provide a means of communication from one computer to another and used to store, transfer and receive data and image files.

8. An “Internet Protocol” (IP) address is a unique series of numbers, separated by a period, that identifies each computer using, or connected to, the Internet over a network. An IP address permits a computer (or other digital device) to communicate with other devices via the Internet. The IP addresses aids in identifying the location of digital devices that are connected to the Internet so that they can be differentiated from other devices. As a mailing address allows a sender to mail a letter, a remote computer uses an IP address to communicate with other computers.

9. An “Internet Service Provider” (ISP) is an entity that provides access to the Internet to its subscribers.

10. Snapchat is a mobile application made by Snap Inc. and available through the iPhone App Store and Google Play. The application provides a way to share moments with photos, videos, and text. A user takes a photo or video using their camera phone in real-time and then selects which of their friends to send the message to. Unless the sender or recipient opts to save the photo or video, the message will be deleted from their devices (after the content is sent in the case of the sender and after it is opened in the case of the recipient). Users are able to save a photo or video they’ve taken locally to their device or to Memories, which is Snapchat’s cloud-storage service. While an official web-based version of Snapchat for PC is not available, users can use Snapchat on a PC by way of an Android emulator. An android emulator is a virtual software that allows you to run an Android device interface on your PC or Mac.



11. Stories: A user can add a photo or video Snaps to their “Story.” Depending on the user’s privacy settings, the photos and videos added to a Story can be viewed by either all Snapchatters or just the user’s friends for up to 24 hours. Stories can also be saved in Memories.

12. Memories: Memories is Snapchat’s cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone’s photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by us and may remain in Memories until deleted by the user.

13. Chat: A user can also type messages, send photos, videos, audio notes, and video notes to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message that they want to keep. The user can clear the message by tapping it again.

### **COMPUTERS AND CHILD PORNOGRAPHY**

14. From my own training and experience in the area of Internet-based child exploitation investigations, and through consultation with other knowledgeable law enforcement officials, I know the following to be true.

15. Computers connected to the Internet identify each other by an IP address. An IP address can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead a law enforcement officer to a particular Internet service company and that company can typically identify the account that uses or used the address to access the Internet.

16. The information contained in this section is based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions.

17. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-based/ subscription-based Web sites to conduct business, allowing them to remain relatively anonymous. Child pornography is also traded through chat rooms and file sharing software.

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography

can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

b. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as America Online (“AOL”) and Microsoft, which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

c. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) Web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and

verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the Web sites and images accessed by the recipient.

d. The computer's capability to store images in digital form makes it an ideal repository for child pornography. Hard drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

#### **PROBABLE CAUSE**

18. On October 13, 2021, a School Resource Officer (SRO) for Manchester Police Department (Manchester, Missouri), within the Eastern District of Missouri, was contacted at Parkway South High School by two minor female students, hereinafter identified as C.D. and J.H.

19. C.D. advised the SRO she wanted to report a 21-year-old adult male, LUKE EDWARD NICOZINSIN (hereinafter "NICOZINSIN"), who had sent her nude photos of his genitals and videos of oral sex. C.D. provided the SRO with the following additional details:

a. C.D. became friends with NICOZINSIN through the online communication application Snapchat.

b. C.D. and NICOZINSIN discussed their ages. NICOZINSIN was 20 at the time and C.D. told NICOZINSIN she was 15. NICOZINSIN responded to learning C.D.'s age by saying it's ok as long as you don't tell anyone.

c. C.D. and NICOZINSIN's friendship became sexual in nature and NICOZINSIN began asking C.D. to send nude pictures to him. NICOZINSIN sent nude pictures of his genitalia to C.D.

d. NICOZINSIN began asking C.D. to meet up for oral sex and eventually, on February 20, 2021, they met in person at NICOZINSIN's residence, the SUBJECT PREMISES. On that date, NICOZINSIN and C.D. had sexual intercourse. C.D. asked NICOZINSIN to wear a condom, but he refused.

e. NICOZINSIN and C.D. engaged in unprotected sex over a dozen times, from February 20, 2021, to October 11, 2021. C.D. kept notes on her phone of her sexual encounters with NICOZINSIN and several other teenage individuals with whom she had had sex.

f. NICOZINSIN recently blamed C.D. for a sexually transmitted disease, so C.D. blocked him on Snapchat and decided to report him.

20. Manchester Police attempted to schedule a child/adolescent forensic interview of C.D. by the Child Advocacy Centers (CAC) of St. Louis. However, due to the volume of cases the CAC was unable to immediately conduct said interview.

21. A limited follow-up interview of C.D. was conducted by a Manchester Police detective to confirm the information provided by C.D. to the SRO. C.D. confirmed the information provided to the SRO and provided the following additional information:

a. C.D. showed the interviewing detective a file on her phone named "Pedo File," where she kept images and videos of her and NICOZINSIN engaging in sex.

b. C.D. advised NICOZINSIN asked to use her phone to take the videos. Most of the videos of C.D. and NICOZINSIN engaging in sex were taken by NICOZINSIN with C.D.'s

phone. However, NICOZINSIN also took videos with his phone. C.D. is aware NICOZINSIN sent some of the videos of them having sex to friends.

c. NICOZINSIN has distinctive moles on his abdomen and there are screenshots on C.D.'s phone in which she has circled those moles.

22. C.D. and C.D.'s parents provided Manchester Police consent to search her smartphone via a Consent to Search Form.

23. A digital forensic extraction was conducted. Due to the volume of data on the device, a review of the data is still ongoing. However, detectives immediately located approximately ten (10) videos on C.D.'s phone, in the file folder specified by C.D., of what is believed to be NICOZINSIN and C.D. engaging in sex acts. Also located on the device were several screenshots clearly taken from said videos as well as some text communications between C.D. and "Luke N."

24. Your Affiant reviewed the referenced videos and screenshots. NICOZINSIN's face was not visible in any of the videos. However, in several of the videos, your Affiant observed two distinct moles on the chest/abdomen of the male depicted in the video.

25. An unrelated image from C.D.'s phone of NICOZINSIN, in which his face was visible, and in which he was shirtless and holding a shotgun, was also viewed by your Affiant. The individual depicted in the image was believed by your Affiant to be a positive match to a Missouri Driver's license photo of NICOZINSIN. Two moles were observed on NICOZINSIN's chest/abdomen that appeared to match with those observed in the sex videos viewed by your Affiant. Said moles were circled, as C.D. had indicated to Manchester Police

26. One of the ten videos purported to be of NICOZINSIN and C.D. engaging in sex, filename IMG8653, is approximately 14 seconds in length and clearly depicts C.D.'s face, as she is on her knees performing oral sex on an adult male. The adult male's pelvic area and legs/feet are visible in the video, but his face, chest and abdomen are not visible. Based on the camera angle, your Affiant believes that the video was taken by the adult male.

27. Your Affiant reviewed a text message string that occurred from September 30, 2021, to October 2, 2021, between C.D. and "Luke N," in which "Luke N" asks about having sex with C.D.'s (unidentified) friend. C.D. tells "Luke N" her friend "might not fuck" because of an infection. "Luke N" then asks if he and C.D. can still have sex. They discuss getting together to have sex at the park. C.D. confirms she has arrived at the park and "Luke N" directs her to the bathroom by the playground. On the following day "Luke N" asks C.D., "Give me pussy after school?". C.D. responds that she didn't go to school because she doesn't feel good in the head and is throwing up from anxiety.

28. The following information was provided by fifteen-year-old minor female J.H. to the Manchester Police Department SRO on October 13, 2021:

a. J.H. advised that NICOZINSIN had also sent her (nude) pictures and videos, but she had since deleted them from her phone.

b. J.H. posted on her Snapchat "My Story" for girls to watch out for NICOZINSIN because he is a pedophile.

c. J.H. advised that a middle schooler had told her something disturbing about NICOZINSIN. J.H. told the SRO that J.H. had promised not to tell but decided it was the right thing to do. J.H. showed the SRO a screenshot of a conversation on Snapchat with another user,

later identified as a twelve-year-old minor female, hereinafter referred to as S.M. J.H. identified S.M. as just a friend she made on Snapchat.

d. The referenced screenshot of the Snapchat message from S.M. stated: “He begged me and my friends for head and drove to a parking lot for it and waited 45 minutes when we told him to leave, then he sent me multiple pictures of his dick that were unwanted. I have screenshots of him getting head as well because he sent that too me too and he still asked me for nudes after I told him I was a minor.”

29. While conducting their initial investigation, Manchester Police became aware NICOZINSIN had been arrested by Chesterfield Police Department (Chesterfield, Missouri) in July 2021 for child molestation involving a 14-year-old minor female, hereinafter identified as E.O. An ex parte order of protection order was subsequently filed restraining NICOZINSIN from contacting and/or being within 100 feet of E.O.

30. On July 28, 2021, E.O. reported to a school official she had been sexually assaulted the prior evening (July 27, 2021). Chesterfield Police were contacted and the responding officer was provided the following information by E.O:

a. E.O. was at a local movie theater the previous evening with her school band group when the assault occurred.

b. E.O. had met NICOZINSIN on Snapchat approximately 2-3 months prior.

c. E.O. and NICOZINSIN talked for a few weeks, then NICOZINSIN began to solicit nude photos from her. E.O. sent NICOZINSIN approximately 5 photos of her nude breasts and buttocks.



d. NICOZINSIN became pushy and demanding about wanting to meet up so she blocked him on Snapchat. She added him back as a Snapchat friend a few weeks later, not immediately realizing it was him because of a different screen name.

e. E.O. told NICOZINSIN she would be at a movie theater on July 27, 2021, and invited him to come see her.

f. NICOZINSIN came to the movie theater and met E.O. They went into a men's restroom at the theater and NICOZINSIN became pushy and demanding. E.O. performed oral sex on NICOZINSIN and he said he wanted to have vaginal sex. E.O. told him no, unless he wore a condom. After having vaginal sex, NICOZINSIN removed the condom so E.O. could perform oral sex on him again. NICOZINSIN and E.O. then had vaginal sex again but E.O. did not realize NICOZINSIN was not wearing a condom. NICOZINSIN ejaculated on her buttocks

g. E.O. went back into the movie theater and told her friends what had happened. E.O. told the responding Chesterfield Officer she was upset NICOZINSIN did not wear a condom and did not feel right about it. E.O. reiterated she had told NICOZINSIN no when he was initially not wearing a condom.

h. E.O. reported she had just lost her virginity the same evening at the movie theater with an 18-year-old black male, who E.O. described as a friend. The sex was consensual and the identified 18-year-old male wore a condom. It occurred in the same restroom just before E.O. had sex with NICOZINSIN.

31. Chesterfield Police Department obtained video surveillance footage from Marcus Theaters for the evening of July 27, 2021. A review of the footage confirmed it to be consistent with E.O.'s statement. E.O. was first observed with an individual who matched the descriptors of

the 18-year old male. They entered the men's restroom and came out a short while later, at which time E.O. engaged with NICOZINSIN and entered the men's restroom with him.

32. On July 29, 2021, a detective from Chesterfield Police Department contacted NICOZINSIN about submitting for an interview. NICOZINSIN ultimately declined to be interviewed through his attorney. On July 30, 2021, NICOZINSIN was arrested by Chesterfield Police Department on a charge of 4<sup>th</sup> degree child molestation. NICOZINSIN did not have a smartphone on his person at the time of arrest. NICOZINSIN was booked and released pending application for a warrant. A warrant has not yet been issued.

33. Open source, private source and Missouri Department of Revenue database checks by Manchester Police Department and by your Affiant identified LUKE EDWARD NICOZINSIN, date of birth XX/XX/2000, current residential address as the SUBJECT PREMISES. A 2003 Nissan 350, Missouri plate FR0H4N, tag expiration August 2021, was registered to NICOZINSIN at the SUBJECT PREMISES. NICOZINSIN's driver's license was suspended on or around June 5, 2021, due to excessive points and failure to maintain proof.

34. NICOZINSIN's Facebook page, which has the display name Luke Nicozinsin and contains a homepage photo and many additional images of LUKE EDWARD NICOZININ, has numerous pictures of a Nissan 350. One such picture depicts NICOZINSIN standing in front of the vehicle. A large caption is visible across the top of the vehicle's front windshield that reads "SEND NUDES."

35. On October 19, 2021, your Affiant conducted spot checks/surveillance at the SUBJECT PREMISES. A Nissan 350 was not observed in the driveway or nearby street. Your Affiant discovered that a St. Louis County Police Officer lives nearby and contacted the officer,

who confirmed he has recently seen NICOZINSIN and that NICOZINSIN currently resides at the SUBJECT PREMISES with his family. The officer further advised NICOZINSIN keeps his Nissan 350 in the garage.

36. As detailed in the Computers and Child Pornography section of this affidavit, computers and the Internet make it easy to share information between devices. Additionally, based on training and experience, your Affiant is aware collectors of child pornography often transfer and store child pornography on multiple devices and media.

37. Based on the foregoing your affiant submits there is probable cause to believe evidence of production and/or possession of child pornography, online enticement, and/or solicitation of sex with a minor is located on electronic devices and storage media owned and/or controlled by NICOZINSIN, at the SUBJECT PREMISES.

#### **SEIZURE OF EQUIPMENT AND DATA**

38. Based upon my knowledge, training and experience, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with

deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process may take weeks or months, depending on the volume of data stored and it would be impractical to attempt this kind of data analysis on-site.

b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even “hidden”, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

39. Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under appropriate circumstances, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus

subject to immediate seizure as such-- or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readable, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

40. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - - for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to

retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

41. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel with whom I have spoken, I am aware that searches and seizures of evidence from computers taken from the subject premises commonly require agents to seize most or all of a computer system's input/output peripheral devices, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the subject premises, and in order to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPU) and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, such materials and/or equipment will be returned within a reasonable time.

42. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an

individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

#### **SEARCH METHODOLOGY TO BE EMPLOYED**

43. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer system(s) and computer hardware to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s);
- b. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth

herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- d. surveying various file directories and the individual files they contain;
- e. opening files in order to determine their contents;
- f. scanning storage areas;
- g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

#### **USE OF BIOMETRIC FEATURES TO UNLOCK ELECTRONIC DEVICES**

44. The warrant I am applying for would permit law enforcement to compel **NICOZINSIN** to unlock a device subject to seizure pursuant to this warrant that is his possession or for which law enforcement otherwise has a reasonable basis to believe is used by him using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition



features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. I have probable cause to believe that one or more of the electronic devices in the SUBJECT PREMISES are likely to offer its user the ability to use biometric features to unlock the device(s). Your affiant knows that many smart phones use fingerprint sensor technology and facial recognition to unlock the phone.

c. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

d. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

e. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

f. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

g. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

h. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that

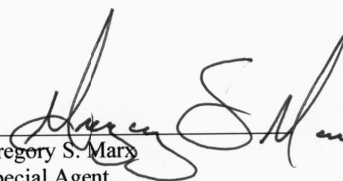
biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

45. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, and the device is in **NICOZINSIN**'s possession or law enforcement otherwise has a reasonable basis to believe is used by **NICOZINSIN**, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of **NICOZINSIN**, to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of **NICOZINSIN**, and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of **NICOZINSIN**, and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

**CONCLUSION**

46. Based on the above information, there is probable cause to believe that the SUBJECT OFFENSES have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES described in Attachment A, and any computers, computer media, or wireless telephones therein, and more fully described herein. Your Affiant requests authority to seize such material, specifically, that the Court issue a search warrant for these premises and all computers, computer hardware and media, and wireless telephones therein.

**I state under the penalty of perjury that the foregoing is true and correct.**

  
Gregory S. Marx  
Special Agent  
Federal Bureau of Investigation

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to  
Federal Rules of Criminal Procedure 4.1 and 41 on October 20, 2021.

  
Hon. Stephen R. Welby  
United States Magistrate Judge

**ATTACHMENT A**  
**DESCRIPTION OF LOCATION TO BE SEARCHED**

The property to be searched is the premises located at: 276 ASPEN VILLAGE DR., BALLWIN, MISSOURI 63021 (the “SUBJECT PREMISES”), further described as: a single-family residence, with “276” clearly marked on the mailbox and above the garage door, and includes the residential building, any vehicles in the garage and/or driveway (including but not limited to a 2003 Nissan 350, Missouri plate FR0H4N) and further described in the photograph as follows:



**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

All records, items, and information relating to violations of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422, that constitute fruits, evidence and instrumentalities of those violations involving of including **LUKE EDWARD NICOZINSIN** (“**NICOZINSIN**”), including:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt or storage of the same, including but not limited to:

- a. Any computer, cell phone, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices) (hereinafter referred to collectively as Devices);
- b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and
- c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer and cell phone passwords and other data security devices designed to restrict access to or hide computer or cell phone software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, materials, emails, and/or internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.

4. Any and all records, documents, records, materials, invoices, notes and/or materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

5. Any evidence of sexual activity involving a minor.

6. Documents, records and/or materials regarding the ownership and/or possession of the SUBJECT PREMISES.

7. During the course of the search, photographs and/or videos of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein.

8. During the execution of the search of the SUBJECT PREMISES, law enforcement personnel are also specifically authorized to obtain from **NICOZINSIN**, if he is on the SUBJECT PREMISES at the time of execution of the warrant, the display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any electronic device, such as, but not limited to computers, computer hardware, cell phones, and tablets, requiring such biometric access subject to seizure pursuant to this warrant, that is, including pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- (a) any of the Device(s) found at the SUBJECT PREMISES that are in the possession of, or known to be used by, **NICOZINSIN**,



- (b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the electronic device(s)'s, which include, but are not limited to, computers, computer hardware, cell phones, and tablets, security features in order to search the contents as authorized by this warrant.

The terms “records,” “documents,” and “materials,” as used in Attachment B, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

As used in Attachment B, the term computer includes cellular telephones/smartphones.